# vEdge의 NTP(Network Time Protocol) 문제 해결

## 목차



## 소개

이 문서에서는 vEdge 플랫폼에서 show ntp 명령 및 패킷 캡처 툴을 사용하여 NTP(Network Time Protocol) 문제를 해결하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

이 문서에 대한 특정 요건이 없습니다.

### 사용되는 구성 요소

이 문서는 특정 소프트웨어 버전 또는 vEdge 모델에 국한되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## NTP 문제의 증상 예

vEdge에 대한 NTP 동기화 손실은 다음과 같은 몇 가지 방법으로 나타날 수 있습니다.

- 디바이스의 show clock 출력에 잘못된 시간이 있습니다.
- 인증서가 유효 범위를 벗어난 잘못된 시간으로 인해 유효하지 않은 것으로 표시됩니다.
- 로그의 타임스탬프가 잘못되었습니다.

# NTP show 명령

NTP 문제의 격리를 시작하려면 두 가지 기본 명령의 사용 및 출력을 이해해야 합니다.

- ntp 연결 표시
- show ntp peer

특정 명령에 대한 자세한 내용은 SD-WAN Command Reference(SD-WAN 명령 참조)를 참조하십시오.

## NTP 연결 표시

```
vedge1# show ntp associations

                                                                    LAST
IDX  ASSOCID  STATUS  CONF  REACHABILITY  AUTH  CONDITION  EVENT      COUNT
------------------------------------------------------------------------------
1    56368    8011    yes   no            none  reject     mobilize   1
2    56369    911a    yes   yes           none  falsetick  sys_peer   1
3    56370    9124    yes   yes           none  falsetick  reachable  2
```

| | |
|---|---|
| IDX | 로컬 인덱스 번호 |
| 아소시드 | 연결 ID |
| 상태 | 피어 상태 단어(16진수) |
| 회의 | 컨피그레이션(영구 또는 임시) |
| 연결성 | 연결 가능성(예 또는 아니요) |
| 인증 | 인증(ok, yes, bad 또는 none) |
| 조건 | 선택 상태 |
| 이벤트 | 이 피어의 마지막 이벤트 |
| 카운트 | 이벤트 수 |

## NTP 피어 표시

```
vedge1# show ntp peer | tab

INDEX  REMOTE          REFID     ST  TYPE  WHEN  POLL  REACH  DELAY    OFFSET   JITTER
------------------------------------------------------------------------------------
1      192.168.18.201  .STEP.    16  u     37    1024  0      0.000    0.000    0.000
```

```
2       x10.88.244.1    LOCAL(1)  2   u     7     64    377    108.481  140.642  20.278
3       x172.18.108.15  .GPS.     1   u     66    64    377    130.407  -24883.  55.334
```

| | |
|---|---|
| 색인 | 로컬 인덱스 번호 |
| 원격 | NTP 서버 주소 |
| 수정 | 피어의 현재 동기화 원본 |
| ST | 지층<br><br>NTP는 시스템이 신뢰할 수 있는 시간 소스에서 얼마나 떨어져 있는지(NTP 홉 단위)를 설명하기 위해 계층 개념을 사용합니다. 예를 들어, 계층 1 시간 서버에는 무선 장치 또는 원자 클럭이 직접 연결되어 있습니다. NTP를 통해 계층 2 시간 서버로 시간을 보내고, 계층 16까지 보냅니다. NTP를 실행하는 시스템은 통신할 수 있는 계층 번호가 가장 낮은 시스템을 자동으로 선택하고 NTP를 시간 소스로 사용합니다. |
| 유형 | 유형 |
| WHEN | 피어에서 마지막 NTP 패킷이 수신된 이후의 시간이 초 단위로 보고됩니다. 이 값은 폴링 간격보다 작아야 합니다. |
| POLL | 폴링 간격(초) |
| REACH | reach, 마지막 8개 연결 기준 8진수로 지정<br><br>377 (1 1 1 1 1 1 1 1) - 지난 8개 모두 정상<br><br>376 (1 1 1 1 1 1 1 0) - 마지막 연결 불량<br><br>....<br>177 (0 1 1 1 1 1 1 1) - 가장 오래된 연결이 잘못됨, 모두 이후 정상<br>기타 |
| DELAY | 피어에 대한 왕복 지연은 밀리초 단위로 보고됩니다. 클럭을 더 정확하게 설정하기 위해 클럭 시간을 설정할 때 이 delay 값을 고려합니다. |
| OFFSET | offset(밀리초)<br><br>Offset은 피어 간 또는 기본 및 클라이언트 간의 클럭 시간 차이입니다. 이 값은 동기화를 위해 클 |

| | |
|---|---|
| | 라이언트 클럭에 적용되는 수정입니다. 양수 값은 서버 클럭이 더 높음을 나타냅니다. 음수 값은 클라이언트 클럭이 더 높음을 나타냅니다. |
| 지터 | 지터(밀리초) |

# vManage 및 패킷 캡처 툴을 사용하여 NTP 문제 해결

## vManage에서 플로우 시뮬레이션으로 이그레스 확인

1. Monitor(모니터) > Network(네트워크)를 통해 Network Device(네트워크 디바이스) 대시보드를 선택합니다
2. 해당 vEdge를 선택합니다.
3. Troubleshooting(문제 해결) 옵션, Simulate Flows(플로우 시뮬레이트)를 클릭합니다.
4. 드롭다운에서 소스 VPN 및 인터페이스를 지정하고, 목적지 IP를 설정하고, 애플리케이션을 ntp로 설정합니다.
5. 시뮬레이션을 클릭합니다.

이렇게 하면 vEdge의 NTP 트래픽에 대한 예상 포워딩 동작이 제공됩니다.

## vEdge에서 TCPDump 수집

NTP 트래픽이 vEdge의 컨트롤 플레인을 통과할 때 TCPdump를 통해 캡처할 수 있습니다.  일치 조건은 특히 NTP 트래픽을 필터링하기 위해 표준 UDP 포트 123을 사용해야 합니다.

tcpdump vpn 0 옵션 "dst port 123"

```
vedge1# tcpdump interface ge0/0 options "dst port 123"
tcpdump -p -i ge0_0 -s 128 dst port 123 in VPN 0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge0_0, link-type EN10MB (Ethernet), capture size 128 bytes
19:05:44.364567 IP 192.168.19.55.ntp > 10.88.244.1.ntp: NTPv4, Client, length 48
19:05:44.454385 IP 10.88.244.1.ntp > 192.168.19.55.ntp: NTPv4, Server, length 48
19:05:45.364579 IP 192.168.19.55.ntp > 172.18.108.15.ntp: NTPv4, Client, length 48
19:05:45.373547 IP 172.18.108.15.ntp > 192.168.19.55.ntp: NTPv4, Server, length 48
19:06:52.364470 IP 192.168.19.55.ntp > 10.88.244.1.ntp: NTPv4, Client, length 48
19:06:52.549536 IP 10.88.244.1.ntp > 192.168.19.55.ntp: NTPv4, Server, length 48
19:06:54.364486 IP 192.168.19.55.ntp > 172.18.108.15.ntp: NTPv4, Client, length 48
19:06:54.375065 IP 172.18.108.15.ntp > 192.168.19.55.ntp: NTPv4, Server, length 48
```

NTP 패킷 내에서 타임스탬프를 디코딩하려면 verbose flag-v를 추가합니다.

tcpdump vpn 0 옵션 "dst port 123 -v"

```
vedge1# tcpdump interface ge0/0 options "dst port 123 -n -v"
tcpdump -p -i ge0_0 -s 128 dst port 123 -n -v in VPN 0
```

```
tcpdump: listening on ge0_0, link-type EN10MB (Ethernet), capture size 128 bytes
19:10:13.364515 IP (tos 0xb8, ttl 64, id 62640, offset 0, flags [DF], proto UDP (17), length 76)
    192.168.19.55.123 > 192.168.18.201.123: NTPv4, length 48
        Client, Leap indicator: clock unsynchronized (192), Stratum 3 (secondary reference), poll 6 (64
        Root Delay: 0.103881, Root dispersion: 1.073425, Reference-ID: 10.88.244.1
          Reference Timestamp:  3889015198.468340729 (2023/03/28 17:59:58)
          Originator Timestamp: 3889019320.559000091 (2023/03/28 19:08:40)
          Receive Timestamp:    3889019348.377538353 (2023/03/28 19:09:08)
          Transmit Timestamp:   3889019413.364485614 (2023/03/28 19:10:13)
            Originator - Receive Timestamp:  +27.818538262
            Originator - Transmit Timestamp: +92.805485523
19:10:13.365092 IP (tos 0xc0, ttl 255, id 7977, offset 0, flags [none], proto UDP (17), length 76)
    192.168.18.201.123 > 192.168.19.55.123: NTPv4, length 48
        Server, Leap indicator:  (0), Stratum 8 (secondary reference), poll 6 (64s), precision -10
        Root Delay: 0.000000, Root dispersion: 0.002166, Reference-ID: 127.127.1.1
          Reference Timestamp:  3889019384.881000144 (2023/03/28 19:09:44)
          Originator Timestamp: 3889019413.364485614 (2023/03/28 19:10:13)
          Receive Timestamp:    3889019385.557000091 (2023/03/28 19:09:45)
          Transmit Timestamp:   3889019385.557000091 (2023/03/28 19:09:45)
            Originator - Receive Timestamp:  -27.807485523
            Originator - Transmit Timestamp: -27.807485523
```

### vManage에서 Wireshark 캡처 수행

vManage에서 패킷 캡처가 활성화된 경우 NTP 트래픽도 이러한 방식으로 Wireshark에서 읽을 수 있는 파일에 직접 캡처할 수 있습니다.

1. Monitor(모니터) > Network(네트워크)를 통해 Network Device(네트워크 디바이스) 대시보드를 선택합니다
2. 해당 vEdge를 선택합니다.
3. Troubleshooting(문제 해결) 옵션, Packet Capture(패킷 캡처)를 차례로 클릭합니다.
4. 드롭다운 메뉴에서 VPN 0 및 외부 인터페이스를 선택합니다.
5. Traffic Filter를 클릭합니다. 여기서 대상 포트 123을 지정하고 필요한 경우 특정 대상 서버를 지정할 수 있습니다.

---

참고: Filter by IP address(IP 주소별 필터)는 소스 또는 대상별로 IP 필터가 있으므로 한 쪽 방향으로만 패킷을 캡처합니다. 목적지 레이어 4 포트는 양방향으로 123이므로 양방향 트래픽을 캡처하기 위해서만 포트로 필터링합니다.

---

6. 시작을 클릭합니다.

이제 vManage는 vEdge와 통신하여 5분 동안 또는 5MB 버퍼가 가득 찰 때까지(둘 중 먼저 오는 값) 패킷 캡처를 수집합니다. 완료되면 해당 캡처를 다운로드하여 검토할 수 있습니다.

## 일반적인 NTP 문제

### NTP 패킷이 수신되지 않음

패킷 캡처는 구성된 서버로 전송된 아웃바운드 패킷을 표시하지만 수신된 회신은 없습니다.

```
vedge1# tcpdump interface ge0/0 options "dst 192.168.18.201 && dst port 123 -n"
tcpdump -p -i ge0_0 -s 128 dst 192.168.18.201 && dst port 123 -n in VPN 0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge0_0, link-type EN10MB (Ethernet), capture size 128 bytes
14:24:49.364507 IP 192.168.19.55.123 > 192.168.18.201.123: NTPv4, Client, length 48
14:25:55.364534 IP 192.168.19.55.123 > 192.168.18.201.123: NTPv4, Client, length 48
14:27:00.364521 IP 192.168.19.55.123 > 192.168.18.201.123: NTPv4, Client, length 48
^C
3 packets captured
3 packets received by filter
0 packets dropped by kernel
```

NTP 패킷이 수신되지 않음을 확인한 후 다음을 수행할 수 있습니다.

- NTP가 올바르게 설정되었는지 확인합니다.
- 트래픽이 VPN 0에서 터널을 통과하는 경우 터널 인터페이스에서 allow-service ntp 또는 allow-service all이 활성화되었는지 확인합니다.
- NTP가 액세스 목록 또는 중간 디바이스에 의해 차단되는지 확인합니다.
- NTP 소스와 대상 간의 라우팅 문제를 확인합니다.

## 동기화 손실

서버에 대한 분산 및/또는 지연 값이 매우 높아질 경우 동기화 손실이 발생할 수 있다. 값이 높으면 패킷이 서버/피어에서 클라이언트에 도달하는 데 시간 루트를 기준으로 너무 오래 걸린다는 것을 나타냅니다. 따라서 로컬 시스템은 패킷에 있는 시간의 정확성을 신뢰할 수 없습니다. 패킷이 도착하는 데 걸린 시간을 알 수 없기 때문입니다.

경로에 버퍼링을 유발하는 혼잡한 링크가 있는 경우 패킷이 NTP 클라이언트에 오면서 지연됩니다.

동기화 손실이 발생하면 다음 링크를 확인해야 합니다.

- 경로에 혼잡/초과 서브스크립션이 있습니까?
- 삭제된 패킷이 관찰됩니까?
- 암호화가 포함되어 있습니까?

show ntp peer의 reach 값은 NTP 트래픽의 손실을 나타낼 수 있습니다. 값이 377보다 작으면 패킷이 간헐적으로 수신되고 클라이언트가 동기화되지 않습니다.

## 장치의 시계가 수동으로 설정되었습니다.

NTP에서 학습한 클럭 값은 clock set 명령을 통해 재정의할 수 있습니다. 이 경우 모든 피어에 대한 오프셋 값이 크게 증가합니다.

```
vedge1# show ntp peer | tab

INDEX  REMOTE           REFID     ST  TYPE  WHEN  POLL  REACH  DELAY    OFFSET   JITTER
------------------------------------------------------------------------------------------
1      x10.88.244.1     LOCAL(1)  2   u     40    64    1      293.339  -539686  88.035
2      x172.18.108.15   .GPS.     1   u     39    64    1      30.408   -539686  8.768
3      x192.168.18.201  LOCAL(1)  8   u     38    64    1      5.743    -539686  2.435
```

자세한 캡처를 사용하면 참조 타임스탬프와 발신자 타임스탬프가 정렬되지 않습니다.

```
vedge1# tcpdump interface ge0/0 options "src 192.168.18.201 && dst port 123 -n -v"
tcpdump -p -i ge0_0 -s 128 src 192.168.18.201 && dst port 123 -n -v in VPN 0
tcpdump: listening on ge0_0, link-type EN10MB (Ethernet), capture size 128 bytes
00:01:28.156796 IP (tos 0xc0, ttl 255, id 8542, offset 0, flags [none], proto UDP (17), length 76)
    192.168.18.201.123 > 192.168.19.55.123: NTPv4, length 48
        Server, Leap indicator:  (0), Stratum 8 (secondary reference), poll 6 (64s), precision -10
        Root Delay: 0.000000, Root dispersion: 0.002365, Reference-ID: 127.127.1.1
          Reference Timestamp:  3889091263.881000144 (2023/03/29 15:07:43)
          Originator Timestamp: 133810392.155976055 (2040/05/05 00:01:28)
          Receive Timestamp:    3889091277.586000096 (2023/03/29 15:07:57)
          Transmit Timestamp:   3889091277.586000096 (2023/03/29 15:07:57)
            Originator - Receive Timestamp:  -539686410.569975959
            Originator - Transmit Timestamp: -539686410.569975959
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel
```

vEdge가 NTP에 대한 기본 설정을 시간 소스로 다시 시작하도록 하려면 시스템 ntp에서 컨피그레이션을 삭제, 커밋, 다시 추가 및 다시 커밋합니다.

## 참조 및 관련 정보

- NTP 문제 해결 및 디버그(Cisco IOS 디바이스)
- Cisco SD-WAN 명령 참조
- show ntp associations 명령을 사용하여 NTP 상태 확인

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.